REMARKS

In the Office Action of August 24, 2005, the Examiner rejected claims 1-21. Claims 1-21 remain pending in the application. Reconsideration of this application is respectfully requested.

Claim Amendments

Applicants have herein amended claim 1. No new matter is introduced as a result of this amendment, support for which is found within the specification as filed. Applicants respectfully submit that the Examiner's objection and rejections of the pending claims as set forth in the Final Office Action have been overcome and that claims 1 – 21 now pending in the present application are allowable over the cited art for the reasons set forth below.

Rejections – 35 U.S.C. § 103

The Examiner states that certain features upon which Applicants rely (i.e., a portable device that can be directly plugged into a USB socket communicatively coupled to a restricted resource and which has a USB plug integrated into its housing without an intervening cable and capable of coupling the device directly to the USB socket, or the use of such a device in an access control system) are not recited in the claims. Applicants respectfully disagree and submit that those features are already recited in the claims. For example, in claim 1, "a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable access control device directly to the USB socket" has been included as a limitation. In claim 11, "a portable device which can be directly plugged into a universal serial bus (USB) socket communicatively coupled to the restricted resource" and "a USB plug integrated into the housing without an

intervening cable and capable of coupling the portable device directly to the USB socket" have been included as limitations. In claim 17, "directly plugging the portable device into a universal serial bus (USB) socket communicatively coupled to the restricted source" and "a USB plug integrated into the housing without an intervening cable and capable of coupling the portable device directly to the USB socket" have been included as limitations. Accordingly, Applicants submit that the pending claims clearly include all the features upon which Applicants rely.

1. **Rejection of claims 1-8 and 11-21**

The Office rejected claims 1-8 and 11-21 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,088,802 (hereinafter "*Bialick*") in view of U.S. Patent No. 6,385,667 (hereinafter "*Estakhri*"). Applicants respectfully disagree with the Examiner's reading of the disclosures in both *Bialick* and *Estakhri* and submit that *Bialick* and *Estakhri*, alone or in combination, fail to teach or disclose various claimed limitations of the pending claims.

Independent claims 1, 11 and 17

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one or ordinary skill in the art, to modify the reference or to combine the reference teachings. Second there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the

prior art, not in applicant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

It is respectfully submitted that independent claims 1, 11 and 17 are allowable over *Bialick* in view of *Estakhri*, because these references, alone or in combination fail to teach or suggest, among other things, (1) "a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable access control device directly to the USB socket" (Claim 1), (2) "a portable device which can be directly plugged into a universal serial bus (USB) socket communicatively coupled to the restricted resource" and "a USB plug integrated into the housing without an intervening cable and capable of coupling the portable device directly to the USB socket" (Claim 11), and (3) "directly plugging the portable device into a universal serial bus (USB) socket communicatively coupled to the restricted source" and "a USB plug integrated into the housing without an intervening cable and capable of coupling the portable device directly to the USB socket" (Claim 17).

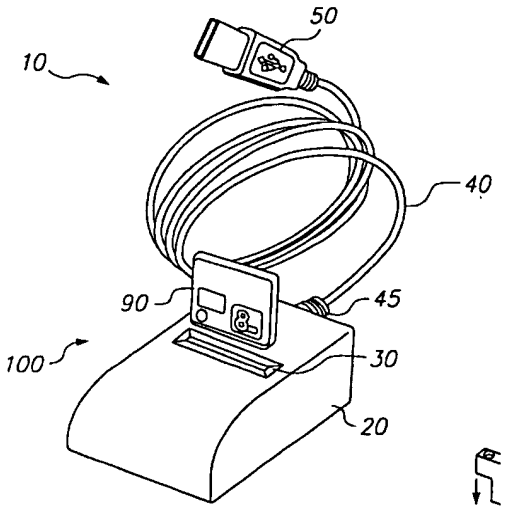
The Examiner cites *Estakhri* for the proposition that it remedies the deficiencies in *Bialick* and further suggests that it is obvious to modify *Bialick* to come up with a device as claimed and that *Estakhri* provides the motivation to do so. Applicants respectfully submit that, as explained below, combining *Bialick* and *Estakhri* would not have been obvious to a skilled artisan and that even if such combination were obvious, *Estakhri* does not disclose the use of an integrated USB plug and thus fails to provide the motivation to modify *Bialick* to remedy at least that deficiency.

It would not have been obvious to a skilled artisan at the time of the invention to combine *Bialick* and *Estakhri* to arrive at the claimed invention in the present application

because *Bialick* and *Estakhri* teach systems geared towards completely opposite objectives. *Bialick* teaches an access control system that serves to restrict access to information stored in a host computer, whereas *Estakhri* teaches an interfacing system that facilitates access to information stored in multiple memory cards. Thus, *Bialick* and *Estakhri* teach two distinct endeavors that seek to achieve opposite results: restricting access to stored information in a host computer versus facilitating access to stored information in multiple memory. The fact that *Bialick* and *Estakhri* refer to flash memory and the USB protocol does not, without more, make the two references combinable. As a result, a skilled artisan would not seek to combine the teachings in *Bialick* and *Estakhri* to come up with the claimed invention in the present application.

Furthermore, *Estakhri* teaches a very different device than that disclosed and claimed in the present application. *Estakhri* teaches a device that allows different memory cards to be used in conjunction with an interface device to facilitate access to information stored in the memory cards. As illustrated in Figure 3, reproduced below, *Estakhri* discloses an interfacing system 300 that can receive a memory card 320 with a 50-pin connection 325 for coupling to a separate interface device 310. Interface device 310 is configurable to various operating modes, each utilizing a different communication protocol. Memory card 320 can likewise be configured to any of various operating modes to match that of interface device 310. When memory card 320 and host computer 335 are connected to interface device 310, host computer 334 can access information stored in memory card 320 via interface device 310. *See, e.g.* col. 5, line 13 to col. 6, line 24.

The Examiner suggests that *Estakhri* teaches a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable data storage device directly to a USB socket on a host computer. Applicants respectfully disagree. Nowhere does *Estakhri* teach a USB plug integrated into the housing of a portable memory device without an intervening cable. Rather, *Estakhri* teaches using a removable memory card in combination with a 50-pin connection as a first interface (element 315) for connection to the removable memory card and at the same time using a second interface (element 314), which can support any of a number of different communication protocols. Furthermore, even in embodiments where the second interface supports a USB plug, *Estakhri* teaches a system wherein the USB plug is connected to the housing via a cable 40, as clearly indicated by Figure 1A of *Estakhri*, reproduced below. Clearly, *Estakhri* does not teach or disclose a USB plug that is integrated into a portable data storage device, which is a required limitation in claims 23 and 24 and which is illustrated in Figure 2 of the Applicants' application, reproduced below.



Estakhri, **Figure 1A**

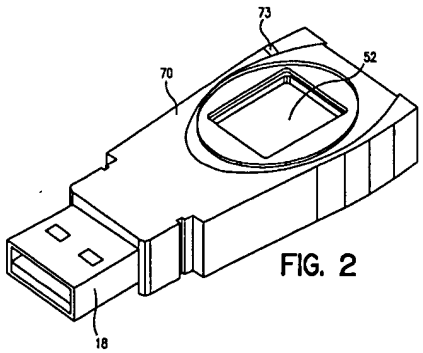


FIG. 2

Applicants' Patent Application, Figure 2

Moreover, *Bialick* fails to disclose the claimed limitations of claim 1 (as amended) which expressly requires the claimed invention to deny user access to the non-volatile memory of the portable device when the biometrics-based authentication module reports a failed user authentication ("said biometrics-based authentication module is configured to grant access to the user data stored in the non-volatile memory provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the user data stored in the non-volatile memory is denied to the user otherwise"). Moreover, none of the disclosures in *Estakhri* remedy this deficiency in *Bialick*.

Applicants respectfully assert that the disclosure in *Bialick* col. 14, lines 50-52 in *Bialick* (using a biometric device "to enable user authentication to a host computing device before allowing access to particular data stored on the host computing device," Col. 14, lines 50-52) fails to teach or disclose using a portable device with biometrics-based authentication capability to control *access to memory in the portable device itself and* the data stored therein, as required by independent claim 1. Controlling access to data stored in a portable device and controlling access to data stored in a host computer to which a portable device is connected are very different. The discussion in *Bialick* fails to teach or disclose a portable device that denies access to memory in the portable device. In fact, as explained below *Bialick* fails to disclose a peripheral device capable of biometrics-based authentication to control access to user data stored in the device's memory.

Bialick discloses a peripheral device with two types of functionalities: (1) security functionality and (2) target functionality. Col. 4, lines 55-65. "Security

functionality" is defined as electronic data security operations such as those that provide maintenance of data confidentiality, data integrity verification, and user authentication. Col. 5, lines 22-28. "Target functionality" is defined to include data storage, enablement of communications from the host device to another device, and the capability to receive and read a smart card inserted in the peripheral device. Col. 4, line 62 through Col. 5, line 4. The peripheral device can be operated in either the security functionality only mode, the target functionality only mode, or the mode wherein both the security functionality and the target functionality are used. Col. 10, lines 13-18.

Bialick defines the use of biometric-based authentication as *a target functionality*, not as a security functionality. *See* Col. 4, line 62 through Col. 5, line 4; Col. 14, lines 10-11, 48-52. Thus, when the peripheral device in *Bialick* is used for biometrics-based authentication, the device cannot be used for other target functionalities such as storage of user data in the device's non-volatile memory. In fact, according to *Bialick*'s disclosures, when the peripheral device includes biometrics capabilities, it is the library of biometric data (such as fingerprint or retinal patterns), not conventional user data, that is stored in the peripheral device's non-volatile memory. Col. 14, lines 57-58. As a result, *Bialick* discloses a biometric device that is used to effectuate user authentication to a host computing device; *Bialick* does not disclose both biometric authentication capabilities and user data storage capabilities in the same peripheral device.

This is in direct contrast to the Applicants' claimed invention, which discloses a portable peripheral device wherein biometric-based authentication is used to control

access to user data stored in the non-volatile memory of the peripheral device. As such, independent claim 1 is patentable over *Bialick* and *Estakhri* at least for these reasons.

For the foregoing reasons, it is respectfully submitted that the combined teachings of *Bialick* and *Estakhri* fail to establish a *prima facie* case of obviousness with regard to the subject matter recited in independent claims 1, 11, and 17. Thus, independent claims 1, 11, and 17 are patentable over the cited references.

Dependent claims 2-8, 12-16 and 18-21

Dependent claims 2-8, 12-16 and 18-21, each being dependent on one of independent claims 1, 11 and 17, are deemed allowable for the same reasons expressed above with respect to independent claims 1, 11 and 17.

Dependent claims 2, 12, and 18 disclose the use of a fingerprint authentication module as the biometrics-based authentication module. The Examiner cites Col. 14, lines 26-28 of *Bialick* and states that *Bialick* teaches a fingerprint authentication module. Applicants respectfully disagree and note that while *Bialick* discloses the use of a fingerprint scanning device, it does not disclose the use of fingerprint scanning in the context of biometric authentication used to grant or deny user access to data stored in the peripheral device or in the context of a device with an integrated USB plug. For these additional reasons, dependent claims 2, 12, and 18 are allowable.

Dependent claims 3 and 13 disclose the use of an iris scan authentication module as the biometrics-based authentication module. The Examiner cites Col. 14, lines 29-33 of *Bialick* and states that *Bialick* teaches an iris scan authentication module. Applicants respectfully disagree and note that while *Bialick* discloses the use of an iris scanning

device, it fails to disclose the use of iris scanning in the context of biometric authentication used to grant or deny user access to data stored in the peripheral device or in the context of a device with an integrated USB plug. For these additional reasons, dependent claims 3 and 13 are allowable.

Dependent claim 4 discloses the biometrics-based authentication module comprised of a biometrics sensor located on one surface of the housing. Dependent claim 14 further discloses said biometrics sensor which is structurally integrated with the portable device is a unitary construction. The Examiner cites Col. 14, lines 48-49 of *Bialick* and states that *Bialick* teaches a biometrics sensor fitted on one surface of the housing and structurally integrated with the portable device in a unitary construction. Applicants respectfully disagree and point out that *Bialick* does not disclose a sensor being fitted on one surface of the portable device or as structurally integrated with the portable device in a unitary construction. For these additional reasons, dependent claims 4 and 14 are allowable.

Dependent claim 5 discloses the use of a non-volatile memory to store biometrics information usable for authentication. Dependent claim 15 further recites the non-volatile memory comprising flash memory. The Examiner cites Figure 8, item 803 and Col. 16, lines 10-11 of *Bialick* and states that *Bialick* discloses the use of non-volatile memory, including flash memory. Applicants respectfully point out that *Bialick* does not disclose such memory in the context of biometric authentication used to grant or deny user access to data stored in the peripheral device or in the context of a device with an integrated USB plug. For these additional reasons, dependent claims 5 and 15 are allowable.

Dependent claims 6, 16 and 21 disclose the use of a bypass mechanism or procedure for authentication as part of the biometrics-based access control system. The Examiner cites col. 10, lines 45-47 of *Bialick* and states that *Bialick* teaches using an acceptable access code such as a password or PIN before allowing access. The Examiner also states that it is obvious to modify *Bialick* to provide a bypass mechanism as claimed and that *Bialick* provides the motivation for such modification. Applicants respectfully disagree and point out that *Bialick* teaches that "the user must successfully enter an acceptable access code (e.g., a password or PIN)..." before being allowed access and that it is desirable to "require an access code before enabling the user to use the security functionality..." (col. 10, lines 46-50). Thus, *Bialick* teaches that the access code be used *in addition to* and *in conjunction with* biometrics-based authentication. In other words, the access code referred to in *Bialick* cannot be a *bypass mechanism*, which by definition is used to bypass, or *in lieu of*, the biometrics authentication. For these additional reasons, dependent claims 6, 16 and 21 are allowable.

Dependent claim 8 recites the restricted resource compromising a communication network. The Examiner cites col. 9, lines 9-11 of *Bialick* and states that *Bialick* discloses that the peripheral device can be made accessible to the host computing device via an appropriate interface such as network connection. The Examiner also states that it is obvious to modify *Bialick* to provide access control to a communication network as claimed and that *Bialick* provides the motivation for such modification. However, *Bialick* neither teaches nor discloses using a portable device to provide access control to a communication network, nor provides any motivation for the modification suggested by the Examiner. While they both interact with a network in operation, a device having

the ability to connect to a network and a device that can provide access control to a communication network are two different devices and entail two distinct endeavors. A device that can connect to a network is not necessarily able to provide access control to a network. Indeed, most are not. For these additional reasons, dependent claim 8 is allowable.

Dependent claim 19 recites the storing of the registered biometrics marker in an encrypted format. The Examiner cites col. 12, lines 12-13 of *Bialick* and states that *Bialick* teaches encrypting and decrypting data stored on the host-computing device. The Examiner also states that it is obvious to modify *Bialick* to encrypt and store the biometrics marker as claimed and that *Bialick* provides the motivation for such modification. Applicants respectfully traverse. As the Examiner has pointed out, in the cited discussion *Bialick* teaches encrypting and decrypting *data stored on the host-computing device*. However, the cited discussion in *Bialick* fails to teach or disclose encrypting and decrypting *data stored in the portable device* as required in the claims. While the use of encryption technique to protect confidential information is well known, performing encryption and decryption on data stored within a portable device and performing such operations on data stored in a host computer to which a portable device is connected are different endeavors. For these additional reasons, dependent claim 19 is allowable.

Dependent claim 20 recites the additional step in the biometrics-based access control method of denying the user access to the restricted source provided that a match between the first biometrics marker and the registered biometrics marker is not identified. The Examiner cites Col. 14, lines 50-52 of *Bialick* and states that *Bialick*

discloses the step of denying the user access provided that a match is not identified. Applicants notes that *Bialick* teaches such a step only in the context of controlling access to a host computing device, rather than to any restricted resource. For these additional reasons, dependent claim 20 is allowable.

2. Rejection of claims 9-10

Claims 9 and 10 stand rejected under 35 U.S.C. § 103 as being unpatentable over *Bialick* in view of U.S. Patent No. 6,219,439 (hereinafter "*Burger*"). Applicants respectfully disagree with the Examiner's reading of the disclosures in both *Bialick* and *Burger* and submit that *Bialick* and *Burger*, alone or in combination, fail to teach or disclose various claimed limitations of claims 9 and 10.

As discussed above, *Bialick* fails to teach or disclose a portable device having an integrated USB plug as claimed and fails to teach or disclose a portable device wherein biometric-based authentication is used to control access to user data stored in the non-volatile memory of the device as claimed. *Burger* does not address these deficiencies in *Bialick*. Accordingly, dependent claims 9 and 10 are patentable over *Bialick* and *Burger*, alone or in combination, at least for this reason.

The Examiner agrees that *Bialick* does not disclose a portable device that can provide access control to a real estate premises that imposes access restrictions or to an operable machinery the safe operation of which requires training, which are claimed in dependent claims 9 and 10 respectively. However, the Examiner then cites *Burger* for the proposition that it remedies these deficiencies in *Bialick*. The Examiner further suggests that it is obvious to modify *Bialick* to come up with a device as claimed and that *Burger* provides the motivation to do so.

However, the statement in *Burger* that the invention therein seeks to "provide for an open, stand-alone system" (col. 3, lines 28-29) does not provide the requisite suggestion or motivation to modify the teaching in *Bialick* with the teaching in *Burger* to arrive at the claimed invention in the present application. A skilled artisan would not seek to combine the teachings in the cited art of record to come up with the claimed invention in the present application. For these additional reasons, dependent claims 9 and 10 are allowable.

CONCLUSION

Applicant asserts that all of the pending claims are patentable over the cited references. A favorable consideration of the present amendment together with the original application is respectfully requested. If the Office desires a telephone conference, the undersigned can be reached at (650) 213-0345.

If there are any additional charges concerning this response, please charge to White & Case LLP Deposit Account 50-3672.

Respectfully submitted,

Dated: September 25, 2006

Thomas V. DelRosario, Reg. No. 46,658
WHITE & CASE LLP
1155 Avenue of the Americas
New York, NY 10036
(650)213-0345